(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平8－55164

(43)公開日　平成８年(1996)２月27日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	17/60				
	13/00	３５１　Ｈ	7368－5E		
		Ｚ	7368－5E		
Ｇ０９Ｃ	1/00		7259－5Ｊ		
				Ｇ０６Ｆ　15/ 21	Ｚ

審査請求　未請求　請求項の数７　書面　（全 12 頁）

(21)出願番号　特願平6－219369

(22)出願日　平成６年(1994)８月10日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

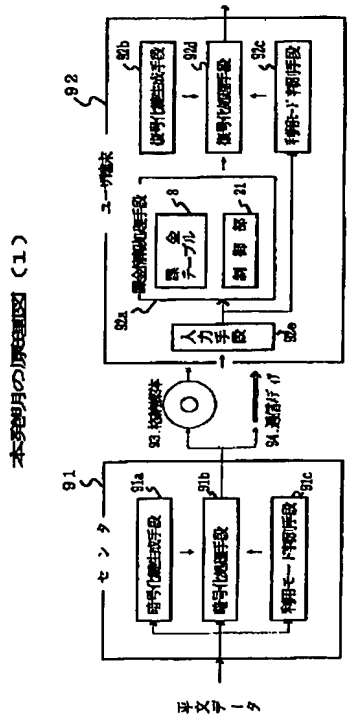
(74)代理人　弁理士　遠山　勉　（外１名）

(54)【発明の名称】　ソフトウェア配送システム、中継装置およびユーザ端末装置

(57)【要約】

【目的】　ソフトウェア格納媒体の販売者と、通信回線を利用してソフトウェアを提供する通信事業者とを含めたソフトウェアの流通形態を実現する。

【構成】　所定のソフトウェアを暗号化してユーザへ提供するセンタとユーザ端末とを備えておき、前記センタおよび中継装置は、ソフトウエア供給形態にとって最適なモードでの暗号化を行うようにした。



1

【特許請求の範囲】

【請求項１】　ソフトウエアを暗号化してユーザ端末に提供し、ユーザはソフトウエアの利用形態に応じて料金を支払うシステムであって、

所定のソフトウェアを暗号化してユーザへ提供するセンタとユーザ端末とを備え、

前記センタは、ユーザが希望するソフトウェアの属性に従って、このソフトウェアを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、

前記ソフトウェアの特性に基づいて暗号化のモードを決定する利用モード判別手段と、

前記暗号化鍵生成手段が生成した暗号化鍵及び前記利用モード判別手段が判別したモードに従って、前記ソフトウェアを暗号化する暗号化処理部とを具備し、

前記ユーザ端末は、前記センタからソフトウェアを提供されたときに、ユーザの課金情報に基づいて前記ソフトウェアの復号化を許可すべき否かを判別する課金情報処理手段と、

前記ソフトウェアの属性に基づいてこのソフトウェアを復号化するための復号化鍵を生成する復号化祖生成手段と、

前記ソフトウェアのモードを判別する利用モード判別手段と、

前記復号化鍵生成手段が生成した復号化鍵及び前記利用モード判別手段が判別したモードに基づいて前記ソフトウェアを復号化する復号化処理手段とを具備することを特徴とするソフトウェア配送システム。

【請求項２】　請求項１において、課金処理手段は、ユーザが利用可能な残高値を登録した課金情報記憶手段と、

前記課金情報記憶手段を参照して残高値が特定値以上であるか否かを判別し、特定値以上ならばデータの復号化を許可すると同時に、前記課金情報記憶手段の残高を減算する制御部とを備えることを特徴とするソフトウェア配送システム。

【請求項３】　請求項１において、前記暗号化鍵生成手段、及び前記復号化鍵生成手段は、前記ソフトウェアを個々に特定するソフトウェアＩＤ、あるいは前記ソフトウェアのタイトルを検出し、これらの情報に基づいて暗号化鍵及び復号化鍵を生成することを特徴とするソフトウェア配送システム。

【請求項４】　請求項１において、前記センタの利用モード判別手段は、前記ソフトウェアのモードを決定する際に、前記ソフトウェアの特性を参照すると同時に、前記ソフトウェアを格納媒体に格納して提供するかあるいは通信を経由して提供するかをを判別し、この判別結果を参照してモードを決定することを特徴とするソフトウェア配送システム。

【請求項５】　請求項１において、前記センタと前記ユーザ端末との間に設けられた中継装置であって、

2

前記中継装置は、前記センタで暗号化されたソフトウェアを復号化するための復号化鍵を生成する復号化鍵生成と、

前記センタから供給されるソフトウェアのモードを判別する入力側利用モード判別手段と、

前記復号化鍵及びモードに基づいて前記ソフトウェアを復号化する復号化処理手段と、

前記復号化されたデータを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、

前記ソフトウェアの特性に基づいて暗号化のモードを決定する出力側利用モード判別手段と、

前記暗号化鍵及び前記モードに基づいて前記ソフトウェアを暗号化する暗号化処理手段とを備えることを特徴とする中継装置。

【請求項６】　前記請求項５の中継装置は、

前記センタから提供されたソフトウェア情報の暗号化モードを判別する利用モード判別手段と、

前記モードに基づいて当該ソフトウェア情報を復号化するための復号化処理手段と、

前記ユーサ端末に提供するソフトウェア情報の提供形態の特性に基づく特有のモードで前記ソフトウエア情報を再度暗号化する暗号化処理手段とを備えていることを特徴とする中継装置。

【請求項７】　通信または媒体で提供された暗号化または非暗号化ソフトウエア情報を再生するとともに、そのソフトウエアの利用に応じた課金を実行するユーザ端末であって、

通信または媒体の種類によって入力経路を切り替える入力切り替え手段と、

暗号化ソフトウエア情報の復号と当該ソフトウエア情報の利用量に応じた課金を管理するソフトウエア管理手段と、

前記ソフトウエア管理手段から出力された復号情報を可視的・可聴的なデータに変換する情報変換部と、

前記ソフトウエア管理手段の前段に設けられ暗号化ソフトウエア情報を前記ソフトウエア管理手段に出力し、非暗号化ソフトウエア情報を前記情報変換部に出力する出力経路切り替え手段とからなるユーザ端末。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、コンピュータプログラムあるいは映像著作物等のソフトウエア、特にデジタル情報化されたソフトウエアの流通システムに適用して有効な技術に関する。

【０００２】

【従来の技術】ＣＤ－ＲＯＭやＭＯ等の大規模記憶媒体や、Ｂ－ＩＳＤＮ等の大容量の高速通信技術、あるいはケーブルテレビ等の技術が発達してくると、これらの手段を用いてコンピュータプログラムは勿論、画像や音声をデジタル情報として流通されることが予想される。

【０００３】すなわち、従来ビデオテープで供給されていたような映像著作物がそのままＣＤ－ＲＯＭ等の格納媒体に格納されて販売されたり、またはＣＤ－ＲＯＭのインタラクティブ性（双方向性）を利用したゲームとして市場に流通し始めてきている。

【０００４】また、通信回線についても同様であり、前記のような映像著作物が通信を経由してユーザの手元に届けられる状況になってきている。ところで、この種のデジタル情報は他の媒体への複写が極めて容易であり、かつアナログ情報のような複写による劣化がないことから、同一情報の複製が可能であり、これらの行為により製造者の利益が害される可能性が極めて高い。すなわち、大容量の書換え可能な光磁気ディスクや磁気ディスク装置さえ所有していればわずかなＤＯＳのコマンドの知識のみでＣＤ－ＲＯＭの内容を複写することが簡単であった。

【０００５】このように、十分なセキュリティチェックが不可能であることを理由にこの種のデジタル情報媒体のレンタル行為は製造者によって禁止されている場合が殆どである。

【０００６】しかしながら、エンドユーザとしては現在のこの種のソフトウエアの価格は高額であり、本当にそのソフトウエアが自身の欲しているものと一致するか、あるいは自身の所有しているハードウエアで使用可能かの確認がとれるまでは購入を躊躇する場合が多い。

【０００７】この点について、機能が制限されている多数のソフトウエアをＣＤ－ＲＯＭに格納して安価に販売し、エンドユーザはその中から希望するソフトウエアについて代金を送金することにより機能制限を解除するコードを通知されるという新しいソフトウエアの流通方式が実現され始めている。

【０００８】また、放送の分野においては、放送局から通信衛星を経由してユーザへ映像著作物を提供する方式が実現されている。この方式では、放送局と契約を交わしているユーザのみに映像著作物を提供するために、通信衛星からユーザに提供する情報を暗号化し、契約ユーザには解読器を提供する。そして、通信衛星から暗号化された情報を復号化するための鍵を送信し、解読器は鍵に基づいて情報を復号化する。これにより、契約ユーザは、復号化された映像情報を家庭用のテレビで視聴することができる。しかし、料金体系は、ユーザの視聴時間等に関係なく、一律の料金を支払う方法を採用しており、さらに、放送というメディアの片方向性によりユーザは放送局が決定した放送プログラムに拘束されるという問題がある。つまり、ユーザは、自身の希望する情報を視聴するためには、放送局が決定した時刻まで待たなければ視聴できないという問題がある。

【０００９】

【発明が解決しようとする課題】そこで、本発明は、少なくとも、画像や音声を提供するセンタと、ＣＤ－ＲＯＭやＭＯ等のソフトウェア格納媒体の販売者と、通信回線を利用してソフトウェアを提供する通信事業者とを含めたソフトウェアの流通形態を実現するために有効な技術を提供し、セキュリティの向上とユーザにかかる時間的な負担の軽減とを図ることを課題とする。

【００１０】

【課題を解決するための手段】本発明は、前記課題を解決するために以下のようにした。これを図１に沿って説明する。

【００１１】先ず、本発明のソフトウェア配送システムは、センタ９１とユーザ端末９２とから構成されている。そして、センタ９１は、ユーザが希望するソフトウェアを暗号化する機能を有している。詳細には、センタは、暗号化鍵生成手段９１ａ、利用モード判別手段９１ｃ、及び暗号化処理手投９１ｂを備えている。

【００１２】暗号化鍵生成手段９１ａは、ソフトウェアを暗号化するための暗号化鍵を生成する機能を有している。利用モード判別手段９１ｃは、ソフトウェアの特性に応じて暗号化のモードを決定する機能を有している。

【００１３】暗号化処理手段９１ｂは、暗号化鍵情報とモードに基づいてソフトウェアを暗号化する機能を有している。次に、ユーザ端末９２は、センタ９１から提供されるソフトウェアを復号化して出力する機能を有している。詳細には、ユーザ端末９２は、課金情報処理手段９２ａ、復号化鍵生成手段９２ｂ、利用モード判別手段９２ｃ、及び復号化処理手段９２ｄを備えている。

【００１４】課金情報処理手段９２ａは、各ユーザが使用できる金額を登録した課金テーブル８（課金情報記憶手段）と、ソフトウェア提供時に課金テーブル８の残高値が特定値以上であるか否かを判別し、特定値以上であれば、ソフトウェアの復号化を許可する制御部９２１とを備えている。

【００１５】さらに、制御部９２１は、復号化を許可したソフトウェアについて、タイトル毎に課金を行う機能を有している。具体的には、ソフトウェアのタイトルを検出し、且つこのタイトルのソフトウェアの復号化を許可する度に、課金テーブル８の残高を減算していく。

【００１６】復号化鍵生成手段９２ｂは、ソフトウェアを復号化するための復号化鍵を生成する機能を有している。利用モード判別手段９２ｃは、センタ９１から提供されたソフトウェアのモードを判別する機能を有している。

【００１７】さらに、復号化処理手段９２ｄは、課金情報処理手段９２ａが復号化を許可した場合に限り、復号化鍵生成手段９２ｂが生成した復号化鍵と利用モード判別手段９２ｃが判別したモードとに基づいてソフトウェアを復号化するものである。

【００１８】また、前述の暗号化鍵生成手段９１ａと復号化鍵生成手段９２ｂとは、個々のソフトウェアを特定するソフトウェアＩＤ、あるいはソフトウェアのタイト

ル等の情報を検出し、これらの情報に基づいて暗号化鍵及び復号化鍵を生成するようにしてもよい。

【００１９】ここで、センタ９１からユーザ端末９２へソフトウェアを提供する方法として、ＣＤ－ＲＯＭやＭＯ等の格納媒体９３にソフトウェアを格納して提供する方法や、通信回線等の通信メディア９４を経由して提供する方法等がある。これに応じて、センタ９１は、ソフトウェアを格納媒体９３へ書き込む機能と、ソフトウェアを送信する機能とを備えるようにする。そして、センタ９１の利用モード判別手段９１ｃは、ソフトウェアを格納媒体９３によりユーザへ提供するのか、あるいは通信メディア９４を介してユーザへ提供するのかを判別し、この判別結果に基づいて暗号化のモードを決定するようにしてもよい。

【００２０】また、本発明のシステムには、センタ９１とユーザ端末９２との間に、図２に示すような中継装置９５を設けるようにしてもよい。この中継装置９５は、センタ９１から格納媒体９３あるいは通信メディア９４を利用して提供されたソフトウェアを、さらに単数または複数のユーザ端末９２へ送信する機能を有している。具体的には、中継装置９５は、復号化鍵生成手段９５ａ、入力側利用モード判別手段９５ｃ、復号化処理手段９５ｂ、暗号化鍵生成手段９５ｄ、出力側利用モード判別手段９５ｃ、暗号化処理手段９５ｆとを備える。

【００２１】ここで、復号化鍵生成手段９５ａは、センタ９１から供給されたソフトウェアを復号化するための復号化鍵を生成する機能を有している。入力側利用モード判別手段９５ｃは、センタ９１から供給されたソフトウェアの暗号化モードを判別する機能を有している。

【００２２】復号化処理手段９５ｂは、復号化鍵生成手段５ａが生成した復号化鍵と入力側利用モード判別手段９５ｃが判別したモードとに基づいてソフトウェアを復号化するものである。

【００２３】暗号化鍵生成手段９５ｄは、復号化されたソフトウェアを暗号化するための暗号化鍵を生成する機能を有している。出力側利用モード判別手段９５ｅは、ソフトウェアの特性に基づいて暗号化のモードを決定するものである。

【００２４】暗号化処理手段９５ｆは、暗号化鍵とモードとに基づいてソフトウェアを暗号化する機能を有している。次に、本発明のユーザ端末について説明する。

【００２５】本発明のユーザ端末９２は、入力装置９２ｅ、課金情報処理手段９２ａ、復号化鍵生成手段９２ｂ、利用モード判別手段９２ｃ、及び復号化処理手段９２ｄを備えている。

【００２６】入力装置９２ｅは、ユーザが希望するソフトウェアを入力するものであり、例えば、格納媒体９３からソフトウェアを読み込むドライブ装置、あるいは通信メディア９４を介して送信されてくるソフトウェアデータを受信する通信装置等である。

【００２７】課金情報処理手段９２ａは、ソフトウェアが入力されたときに、ユーザの課金残高を参照し、ソフトウェアの復号化を許諾するか否かを判別する機能を有している。具体的には、ユーザが使用可能な金額を登録した課金テーブル８と、この課金テーブル８を参照して残高が特定値以上であるか（または”０”でない）否かを判別して特定値以上ならば（”０”でなければ）ソフトウェアの復号化を許可する制御部９２１とを備えている。

【００２８】復号化鍵生成手段９２ｂは、ソフトウェアを復号化するための復号化鍵を生成する機能を有している。具体的には、ソフトウェアのソフトウェアＩＤやタイトル等に基づいて復号化鍵を生成する。

【００２９】利用モード判別手段９２ｃは、入力されたソフトウェアのモードを判別する機能を有している。復号化処理手段９２ｄは、課金情報処理手段９２ａがソフトウェアの復号化を許諾した場合に限り、復号化鍵生成手段９２ｂが生成した復号化鍵及び利用モード判別手段９２ｃが判別したモードに基づいてソフトウェアを復号化する機能を有している。

【００３０】

【作用】本発明のソフトウェア配送システムでは、センタ９１は、ユーザが希望するソフトウェアを暗号化し、ユーザへ提供する。つまり、センタ９１は、ソフトウェアのソフトウェアＩＤやタイトル等に基づいて暗号化鍵を生成すると共に、ソフトウェアのデータ構造等に基づいて暗号化のモードを決定する。そして、センタは、暗号化鍵とモードとに基づいてソフトウェアを暗号化する。

【００３１】センタで暗号化されたソフトウェアは、格納媒体９３や通信メディア９４によりユーザ端末９２へ提供される。ユーザ端末９２では、センタ９１からソフトウェアが提供されたときに、ユーザの課金残高を参照し、残高が特定値以上（”０”でない）ならばソフトウェアの復号化を許諾する。そして、許諾したソフトウェアのタイトル毎にユーザの課金残高を減算する。次に、ユーザ端末９２は、ソフトウェアのソフトウェアＩＤあるいはタイトル等に基づいて復号化鍵を生成すると共に、このソフトウェアのモードを判別する。ユーザ端末９２は、復号化鍵とモードとに基づいてソフトウェアを復号化し、ディスプレイやスピーカ等の出力装置へ出力する。

【００３２】本発明によれば、通信あるいは媒体といったソフトウエアの提供形態がいかなる場合であっても、統一的にソフトウエアの流通を管理することができる。また中継装置を設けて提供形態の変更を可能とすることによって、最適な提供形態でのソフトウエアの流通を実現できる。

【００３３】

【実施例】本実施例において、センタ９１と、中継装置

９５と、ユーザ端末９２とはほぼ同様のハードウエア構成で実現することができる。

【００３４】図３は、その一例としてのユーザ端末の内部構成を機能ブロック図で示したものである。同図において、切り替えスイッチ５７（ＳＷ１）は、入力インターフェースとしても機能し、通信回線５１、ＣＤ－ＲＯＭ５２等の種々の提供経路からのソフトウエア情報を入力する。また、この切り替えスイッチ５７（ＳＷ１）には、図示しない光磁気ディスクドライブ装置を通じて光磁気ディスク５８へのソフトウエア情報の読み書きが可能となっている。

【００３５】切り替えスイッチ５７（ＳＷ１）の次段には、信号処理手段としての受信装置５８、ＭＯ変調器５９およびＣＤ／ＭＯ復調器６０が配置されている。受信装置５８は、通信回線５１からの受信信号として提供されたソフトウエア情報を本装置で取り扱い可能なデータ形式に変換するためのものであり、ＭＯ変調器５９は光磁気ディスク５８への書き込みを行うための変調手段である。また、ＣＤ／ＭＯ復調器６０はＣＤ－ＲＯＭ５２または光磁気ディスク５８からの読み取りデータを復調するためのものであり、制御回路によって復調制御がなされるようになっている。

【００３６】切り替えスイッチ６１（ＳＷ２）は、前記で説明した各信号処理手段から出力されたデータを選択的に各種のエラー処理手段に出力するためのものである。また、光磁気ディスク５８への書き込みを行う場合には、エラー処理手段→信号処理手段への逆力向のデータの転送も制御する。

【００３７】エラー処理手段は、通信系エラー処理部６２と、光磁気ディスク系エラー処理部６２（６２ａ，６２ｂ）と、磁気ディスク・ＣＤ系工ラー処理部６３とに分かれていろ。

【００３８】光磁気ディスク系エラー処理部６２は、エラーチェックコード生成部６２ａと、エラーチェックコード訂正部６２ｂとからなり、光磁気ディスク５８への書き込みを行う場合には前者が機能し、光磁気ディスク５８からの読み出しを行う場合には後者が機能する。なお、磁気ディスク・ＣＤ系エラー処理部６３は、エラーチェックコード訂正とともにビット並び替え等の処理も行うようになっている。

【００３９】前記エラー処理手段の後段には切り替えスイッチ６４（ＳＷ３）が配置されている。この切り替えスイッチ６４（ＳＷ３）は、前記の信号処理手段およびエラー処理手段で処理されたソフトウエア情報を次段のソフトウエア管理部３に出力するか、後述の切り替えスイッチ６５（ＳＷ４）に出力するか、あるいは前述のエラーチェックコード訂正部６２ｂからの出力をエラーチェックコード生成部６２ａに戻すように経路を制御する機能を有している。

（ＣＤ－ＲＯＭ→光磁気ディスクへの書き込み）ここで、切り替えスイッチ６４（ＳＷ３）を制御して、ＣＤ－ＲＯＭ５２から読み込んだ暗号化ソフトウエア情報を光磁気ディスク５８に書き込む手順を簡単に説明する。

【００４０】まず、ＣＤ－ＲＯＭ５２から読み込まれたデータは、切り替えスイッチ５７（ＳＷ１）の経路切り替えによりＣＤ／ＭＯ復調器６０に入力される。ここで復調されたデータは、切り替えスイッチ６１（ＳＷ２）の経路切り替えにより磁気ディスク・ＣＤ系エラー処理部６３に送られる。ここでエラーチェックコード訂正およびビット並び替えが行われたデータは、切り替えスイッチ６４（ＳＷ３）の経路切り替えによってエラーチェックコード生成部６２ａに送られ光磁気ディスクに対応したエラーチェックコードが付加される。そして、このデータは切り替えスイッチ６１（ＳＷ２）の経路切り替えによりＭＯ変調器５９に送られ光磁気ディスク５８に書き込むことのできるデータ形式に変換されて切り替えスイッチ５７（ＳＷ１）を通じて光磁気ディスク５８に書き込まれる。

（ソフトウエア管理部の構成）ソフトウエア管理部３は、モジュール構造でたとえばＩＣカード、ボード等で実現されており、入力用バッファ２１と出力用バッファ２４とを有する復号化部７としてのＤＥＳを中心に構成されている。ここで、ＤＥＳとしては、ＦＩＰ’ＳＰＵＢ社の「４６ＤＡＴＡ　ＥＮＣＲＹＰＴＩＯＮ　ＳＴＡＮＤＡＲＤ　ＮＩＳＴ」を用いることができる。

【００４１】前記ＤＥＳには外部より鍵情報１６が与えられるようになっており、この鍵情報に基づいてＤＥＳが機能して暗号化情報を復号化するようになっている。なお、本実施例においてＤＥＳにはモード判別部１８（ＭＯＤＥ）を有しており、このモード判別部１８は複数のＤＥＳモードの中からそのデータ形式等に対して最適なモードを選択する機能を有している。

【００４２】なお、このＤＥＳは本装置をセンタ９１あるいは中継装置９５として用いる場合には復号化部７（復号か処理手段９５ｂ）としての機能の他、暗号化部（暗号化処理手段９５ｆ）としても機能する。また、このときモード判別部１８は入力側利用モード判別手段９５ｃおよび出力側利用モード判別手段９５ｅとして機能することになる。そして、制御ＣＰＵ４は暗号化鍵生成手段９５ａおよび復号化鍵生成手段９５ｄとして機能することになる。

（ＤＥＳモードの説明）次に前記ＤＥＳモードのうち、代表的なロジックを説明する。なお、以下の説明では復号化処理を中心に説明するが、本装置をセンタ９１または中継装置９５として使用するときには暗号化処理も下記と同様である。

【００４３】図４（ａ）は、ＥＣＢ基本モードであり、ＤＥＳ７において、６４ビットの鍵情報１６により６４ビットの入力データ列を６４ビットの出力データ列として暗号化（または復号化）するモードである。

【００４４】図４（ｂ）は、ＣＢＣモードを示しており、ＤＥＳ７において６４ビットの入力データ列を６４ビットの鍵情報１６で暗号化（または復号化）した後、再度これをＤＥＳ７に帰還入力させる。このようにデータを全て入力し終るまでフィードバックを行い最終結果を出力する方式であり、ファイル等のデータ処理に適している。

【００４５】図４（ｃ）は、ＯＦＢモードを示しており、エラーの生じやすい通信データや、一つの誤りが他に与える影響の大きい音声データ等に適している。図４（ｄ）は、ＣＦＢモードであり、自己同期形のデータに適している。

【００４６】前述のモード判別部１８はモードテーブル２０に格納されたこれらのモードのうちデータ形式等を解析して最適なものを読み出して復号化部（ＤＥＳ）に送出する。ＤＥＳ７ではこのようにして選択されたモードに基づいて暗号化・復号化処理を行う。

（復号化部の詳細）図５は、復号化部７のハードウエア構成を示すブロック図である。

【００４７】同図において、入力側には入力用バッファ２１として、８ビット構成のレジスタが８個接続されて６４ビットのシフトレジスタ（ＲＥＧ１）が配置されており、次段にはセレクタｓｅｌが配置されている。当該セレクタｓｅｌは、後述のＤＥＳ処理メイン回路２５からの出力か、前記シフトレジスタ（ＲＥＧ１）からの出力かを選択的に入力できるようになっている。

【００４８】セレクタｓｅｌの次段には８ビット構成のレジスタ２３（ＲＥＧ２）が配置されさらにその次段にはＤＥＳ処理メイン回路２５が配置されている。このＤＥＳ処理メイン回路２５が復号化部７の中核をなすＤＥＳとして機能する。すなわち、ＤＥＳ処理メイン回路２５には、図４で説明した各種のＤＥＳモードがＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）として登録されており、制御ＣＰＵ４からの指示により最適なＤＥＳモードのロジックを選択して復号処理を行うようになっている。

【００４９】前記ＤＥＳ処理メイン回路２５の出力は前記セレクタｓｅｌと出力用バッファ２４としての出力レジスタ（ＲＥＧ３）に分岐されている。そして出力レジスタ（ＲＥＧ３）の出力が暗号化または復号化されたデータとして用いられる。

【００５０】この処理のシーケンスを示したものが図６である。図６において、入力レジスタ（入力用バッファ２１）の出力は、次サイクルの最初のクロックでレジスタ２３からの出力としてＤＥＳ処理される。そして次のクロックで出力レジスタ（出力用バッファ２４）より出力される。この出力レジスタ（出力用バッファ２４）からの出力時間に入力側では入力レジスタ（入力用バッファ２１）より次サイクルの暗号化データの取り込みが行われている。

【００５１】このように、本実施例では入力用バッファ２１としての入力レジスタ（ＲＥＧ１）と、出力用バッファ２４としての出力レジスタ（ＲＥＧ３）とを独立に設けたことにより、暗号化データの入力と復号化データの出力とをそれぞれ独立して連続的に行うことができるようになった。そのため、従来のＤＥＳのようにサイクリックに入力と出力とを行う場合に較べて高速な復号化・暗号化処理が可能となっている。

【００５２】以上説明したＤＥＳ７は、制御ＣＰＵ４により制御されるようになっており、この制御ＣＰＵ４のバスには前記ＤＥＳ７の他にメモリで構成された課金テーブル８と、インターフェース７２（Ｉ／Ｏ）が接続されている。

【００５３】課金テーブルは８には所定の残高値が登録されており暗号化ソフトウエアデータの復号処理量または処理時間に応じて課金値が減算されるようになっている。残高値を更新したい場合には、カード媒体として提供されているソフトウエア管理モジュールを販売店等に持参し、料金を支払うことにより販売店で課金テーブル８の残高値を増加させることができる。

【００５４】なお、ＳＤ回路３内に課金テーブル８を設けない場合には、当該課金値情報をフロッピーディスク装置等に出力して記録しておく必要がある。この場合に課金値情報をユーザが可読な状態でフロッピーディスク等の媒体に登録しておくとセキュリティが維持できない。そこで、当該課金値等情報のユーザ情報を外部に出力する場合には、前記制御ＣＰＵ４はＤＥＳ７で当該課金値情報を暗号化して暗号データとして出力するようにしてもよい。

【００５５】すなわち、課金値情報を外部に出力する場合には復号化部（ＤＥＳ）は暗号化部として機能することになる。なお、本装置をセンタ９１または中継装置９５としてのみ使用する場合には、このような課金テーブル８は省略してよいことは勿論である。

【００５６】インターフェース７２（Ｉ／Ｏ）はソフトウエア管理部３外のホストＣＰＵ１０と接続されている。なお、前記制御ＣＰＵ４はホスト装置（すなわちソフトウエア従量課金・再生装置本体）側のホストＣＰＵ１０で兼用することも可能である。

【００５７】ホスト側ではホストＣＰＵ１０のバス上にインターフェース（ＩＯ）が接続されており、これと外部インターフェース７５を通じて入力装置７４とモデム７３とが接続されている。

【００５８】ソフトウエア管理部３の出力は、切り替えスイッチ６５（ＳＷ４）を通じて情報変換部である音声画像分離部６６（ＤＥ－ＭＵＸ）、画像伸長部６７ａ，音声伸長部７６ｂ（ＭＰＥＧ）等に出力される。

【００５９】ここで、ＭＰＥＧとしては、チップとして「ＩＳＯ／ＩＥＣ　ＣＤ　１３８１８’１～３」を用いることができる。音声画像分離部６６（ＤＥ－ＭＵＸ）

で分離された画像データは、画像伸長部６７ａ（ＭＰＥＧ）で伸長されＤＡ変換部６８ａで変換されたＮＴＳＣ信号としてＴＶディスプレイ等のアナログ表示機器に出力される。

【００６０】音声伸長部６７ｂ（ＭＰＥＧ）でも同様に音声データが伸長されＤＡ変換部６８ｂで変換されたＮＴ８Ｃ信号としてスピーカ等のアナログオーディオ機器に出力される。そして、画像と音声の同期は同期制御部７０（ＶＲＣ）で制御される。なお、音声画像分離部６６（ＤＥ－ＭＵＸ）の出力をデジタルデータままで外部に出力するときにはインターフェース７１（ＳＣＳＩ）を通じてパーソナルコンピュータ等のデジタル機器に出力する。

【００６１】なお、本装置をセンタ９１または中継装置９５として用いる場合でいわゆるビューワ（コンテンツを参照するツール）を必要としないときには音声画像分離部６６（ＤＥ－ＭＵＸ）以降の構成は省略してもよい。

（本発明におけるソフトウエアの提供ルート）図７～図９を用いて、本発明のソフトウエアの提供モードについて説明する。

【００６２】図７において、センタ９１からエンドユーザ１２１にソフトウエアが提供され得る形態としては、第１に通信事業者１２２を経由するルートがあり、第２にセンタ９１からの直販ルートがあり、第３に販売店１２３を経由するルートがある。

【００６３】第１の通信事業者１２２を経由するルートでは、センタ９１から通信事業者１２２までは通信路Ｃ１でソフトウエアが提供される場合と、媒体形式Ｐ１でソフトウエアが提供される場合がある。通信路Ｃ１としては、公衆回線、光通信路、衛星通信等のあらゆる通信手段を想定することができる。媒体形式Ｐ１としてはｃｄ－ＲＯＭ、光磁気ディスク、ハードディスク、フロッピーディスク等のあらゆる媒体手段を想定することができる。

【００６４】このルートにおいて、通信事業者１２２からエンドユーザ１２１までは通信経路Ｃ２でソフトウエアが提供される。このルートでセンタが通信事業者１２２に対してソフトウエアを提供する場合には、まず通信路Ｃ１の場合には暗号化モードとして図４（ｃ）に示したＯＦＢモードが最も適している。したがって、センタ９１は自身のＤＥＳ７によってＯＦＢモードによる暗号化データを生成し、これを通信路Ｃ１に出力する。

【００６５】通信路Ｃ１から暗号化データを受け取った通信事業者１２２は自身の中継装置９５を用いて受信した暗号化データをそのまま通信路Ｃ２に出力する（図９（ａ））。通信路Ｃ２から暗号化ソフトウエアデータを受け取ったユーザ端末９２の処理は先に説明した通りである。

【００６６】次に、センタ９１から媒体形式で通信事業者１２２に暗号化ソフトウエアデータが送られる場合について説明する。媒体形式Ｐ１の場合には暗号化モードは図４（ｂ）に示したＣＢＣモードが最適である。したがって、センタ９１は自身のＤＥＳ７においてＣＢＣモードでソフトウエアデータを暗号化してＣＤ－ＲＯＭ等の媒体にこのデータを格納する。このように暗号化ソフトウエアデータがＣＤ－ＲＯＭ等の媒体に格納された状態でこれを受領した通信事業者１２２は、この暗号化ソフトウエアデータを通信路Ｃ２に供給するために、自身のＤＥＳ７を用いて暗号化モードの変換を行う（図９（ｂ）参照）。すなわち、先に述べたように通信路Ｃ２に流通させる暗号化モードとしてはＯＦＢモードが適しているため、まず受領した暗号化ソフトウエアデータをＣＢＣモードで復号した後、ＯＦＢモードで再暗号化する。このように暗号化された暗号化ソフトウエアデータを受領したエンドユーザ１２１は、自身のユーザ端末９２のＤＥＳ７で、モード判別部１８（ＭＯＤＥ）で選択されたＯＦＢモードに基づく復号を実行する。

【００６７】次に、販売店１２３を経由したソフトウエアの流通形態について説明する。まずセンタ９１から販売店１２３までが通信路Ｃ３で結ばれており、販売店１２３からエンドユーザ１２１へは媒体形式Ｐ２での提供である場合、センタ９１は自身のＤＥＳ７においてＯＦＢモードで暗号化した暗号化ソフトウエアデータを通信路Ｃ３に送出する。

【００６８】販売店１２３では自身の中継装置９５でこれを受信して光磁気ディスク等の媒体（Ｐ２）にこの暗号化ソフトウエアデータを格納する（図９（ｃ））。この媒体（Ｐ２）の提供を受けたエンドユーザ１２１のユーザ端末９２では、自身のＤＥＳ７においてＯＦＢモードで当該暗号化ソフトウエアデータの復号処理を行う。

【００６９】以上の中継装置９５におけるモード変換の一覧を示したものが図８である。すなわち、以上の説明はいずれも流通方向が片方向（センタ９１からエンドユーザ１２１へ）のみであったが、双方向の場合には全てＣＢＣモードを採用することが望ましい。

【００７０】

【発明の効果】本発明によれば、ソフトウエアの提供形態に最適なモードを選択して暗号化・復号化処理を流通経路上で行うようにしたため、ソフトウェア格納媒体の販売者と、通信回線を利用してソフトウェアを提供する通信事業者とを含めたソフトウェアの流通形態を実現することができる。

【図面の簡単な説明】

【図１】　本発明の原理図（１）

【図２】　本発明の原理図（２）

【図３】　本発明の実施例であるセンタ、中継装置、ユーザ端末のハードウエア構成を示す機能ブロック図

【図４】　ＤＥＳのモードを示す説明図

【図５】　ＤＥＳの詳細を示す説明図

13　　14

【図６】　ＤＥＳの入力と出力のタイミングを示すチャート図

【図７】　本発明のソフトウエアの提供経路を示す説明図

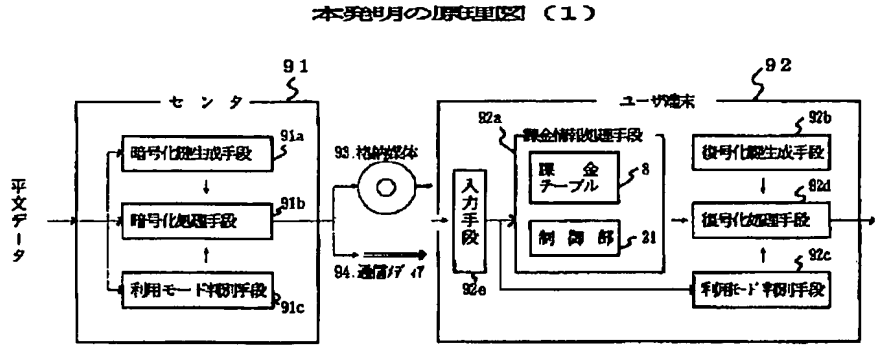
【図８】　提供経路毎のモード変換を示す表図

【図９】　実施例における中継装置でのモード変換を説明するための概念図

【符号の説明】

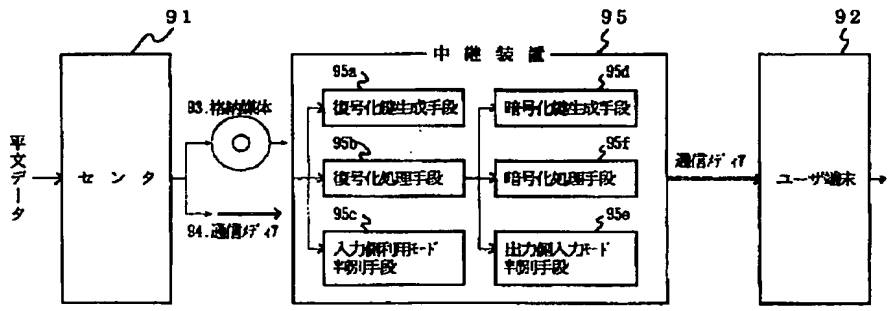
３・・・ソフトウエア管理部、
４・・・制御ＣＰＵ
７・・・ＤＥＳ（復号化部，暗号化部）
８・・・課金テーブル、
１０・・・ホストＣＰＵ
１６・・・鍵情報、
１８・・・モード判別部、
２０・・・モードテーブル、
２１・・・入力用バッファ、
２４・・・出力用バッファ、
５１・・・通信回線、
５７・・・切り替えスイッチ、
５８・・・光磁気ディスク、
５９・・・ＭＯ変調器、
６０・・・ＣＤ／ＭＯ復調器、
６１・・・切り替えスイッチ、
６２・・・通信系エラー処理部、
６２ａ・・・エラーチェックコード生成部、
６２ｂ・・・エラーチェックコード訂正部、
６３・・・磁気ディスク・ＣＤ系エラー処理部、
６４・・・切り替えスイッチ、
６５・・・切り替えスイッチ、
６６・・・音声画像分離部、
６７ａ・・・画像伸長部、
＊６７ｂ・・・音声伸長部、
６８ａ・・・ＤＡ変換部、
６８ｂ・・・ＤＡ変換部、
７０・・・同期制御部、
７１・・・インターフェース、
７２・・・インターフェース、
７３・・・モデム、
７４・・・入力装置、
７５・・・外部インターフェース、
７９・・・受信装置、
９１・・・センタ、
９１ａ・・・暗号化鍵生成手段、
９１ｂ・・・暗号化処理手段、
９１ｃ・・・利用モード判別手段、
９２・・・ユーザ端末、
９２ａ・・・課金情報処理手段、
９２ｂ・・・復号化鍵生成手段、
９２ｃ・・・利用モード判別手段、
９２ｄ・・・復号化処理手段、
９２０・・・入力装置、
９３・・・格納媒体、
９４・・・通信メディア、
９５・・・中継装置、
９５ａ・・・復号化鍵生成手段、
９５ｂ・・・復号化処理手段、
９５ｃ・・・入力側利用モード判別手段、
９５ｄ・・・暗号化鍵生成手段、
９５ｅ・・・出力側利用モード判別手段、
９５ｆ・・・暗号化処理手段、
１０２・・・ソフトウエア管理モジュール、
１０５・・・ソフトウエア従量課金・再生装置、
＊９２１・・・制御部、

【図１】

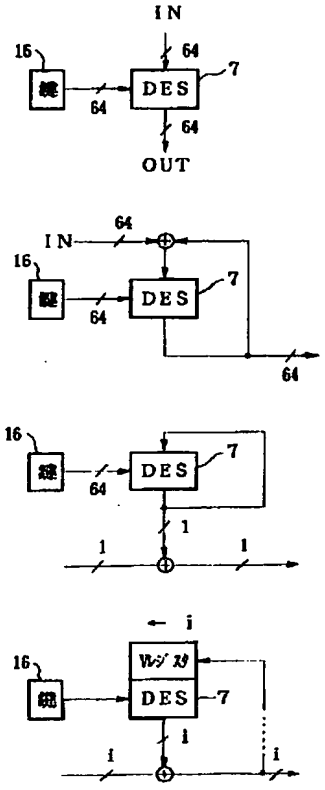


【図２】

本発明の原理図（２）



【図４】



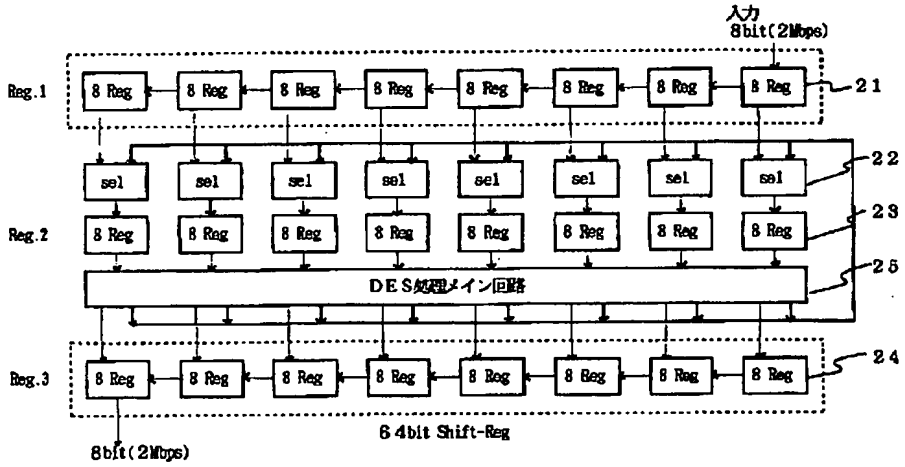
【図８】

提供経路毎のモード変換を示す表図

Cの方式 ルート	C1→C2	P1→C2	C4	C3→P2	P4及びP3→P2
片方向	OFB→OFB	CBC→OFB	OFB	OFB→OFB	CBC→CBC
双方向	CBC→CBC	CBC→CBC	CBC	CBC→CBC	CBC→CBC

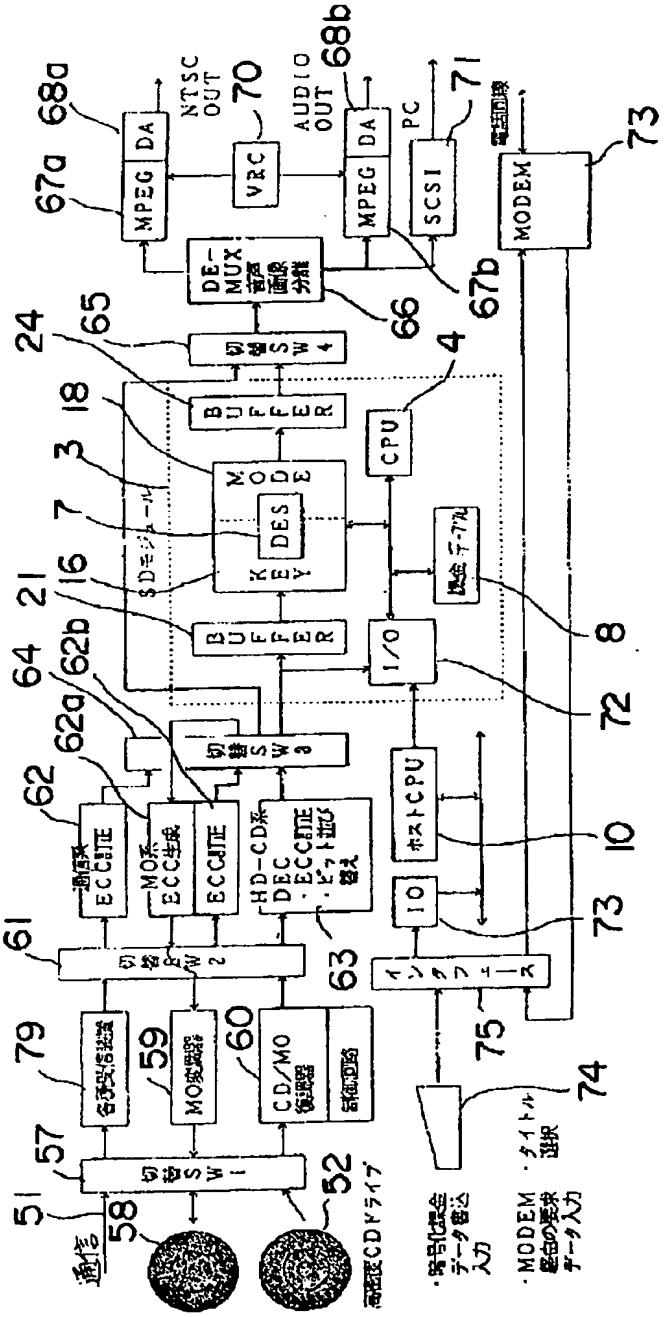
【図５】

実施例のＤＥＳの詳細な構成を示すブロック図



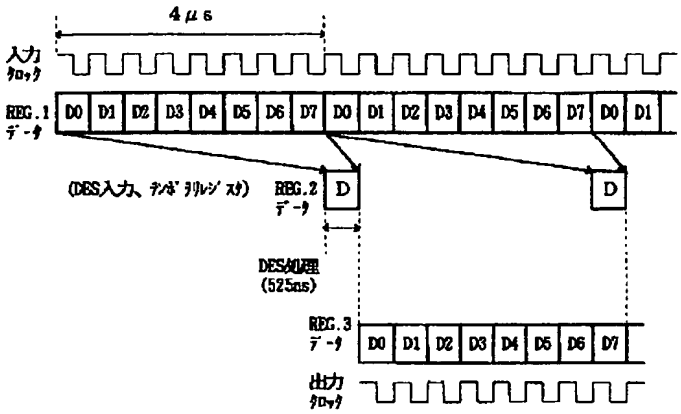
【図３】

本発明の実施例であるソフトウエア従量課金・再生装置の構成を示すブロック図



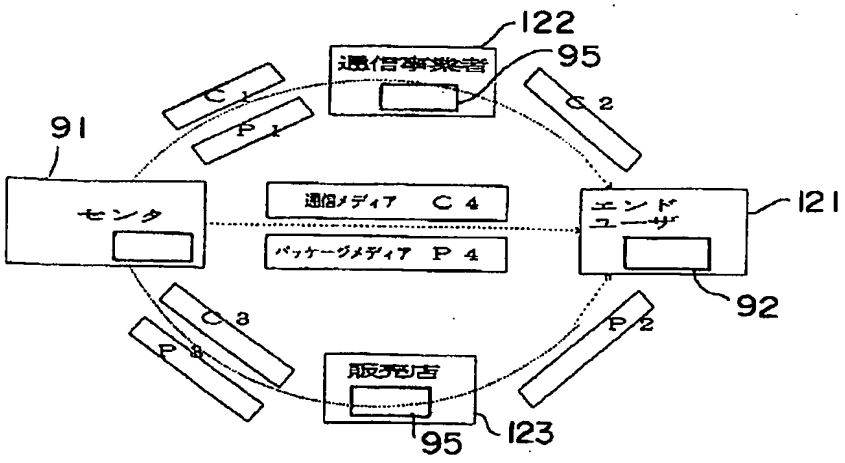
【図６】

実施例のＤＥＳの入力と出力とのタイミングを示すチャート図

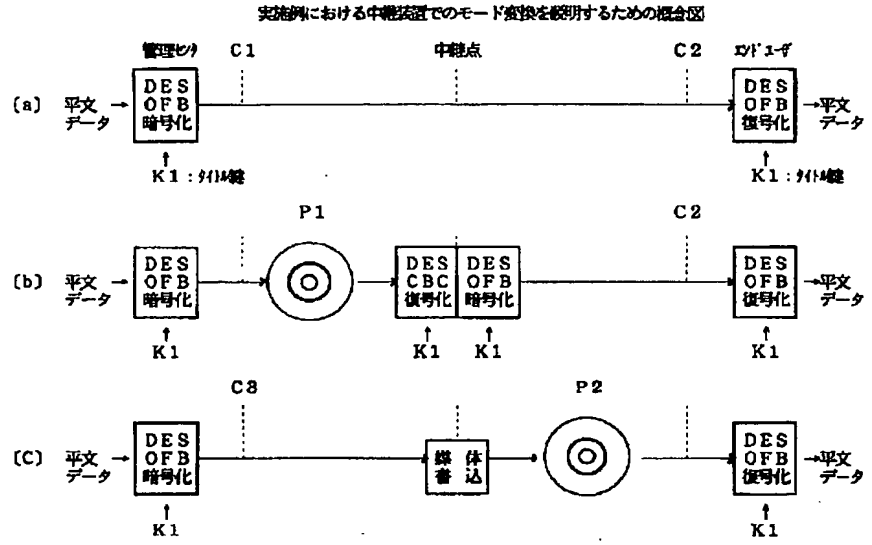


【図７】

本発明のソフトウェアの提供経路を示す説明図



【図９】


実施例における中継装置でのモード変換を説明するための概念図
管理ヒント
C1
中継点
C2
エンドユーザ
(a)
平文データ
DES OFB 暗号化
K1：タイトル鍵
DES OFB 復号化
平文データ
K1：タイトル鍵
P1
C2
(b)
平文データ
DES OFB 暗号化
K1
DES CBC 復号化
K1
DES OFB 暗号化
K1
DES OFB 復号化
K1
平文データ
C3
P2
(C)
平文データ
DES OFB 暗号化
K1
媒体書込
DES OFB 復号化
K1
平文データ